IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of Atty. Docket

MICHAEL A. EPSTEIN PHA 23,637

Serial No.: 09/454,349 Group Art Unit: 3621

Filed: December 3, 1999 Examiner: C.O. Sherr

KEY DISTRIBUTION VIA A MEMORY DEVICE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

APPEAL BRIEF

This is an appeal from the Examiner of Group 3621 finally rejecting claims 1-20 in this application.

(i) Real Party in Interest

The real party in interest in this application is PHILIPS ELECTRONICS NORTH AMERICA CORPORATION by virtue of an assignment from the inventors recorded on December 3, 1999, at Reel 10449, Frames 0402-0403.

(ii) Related Appeals and Interferences

There are no other appeals and/or interferences related to this application.

(iii) Status of the Claims

Claims 1-20 stand finally.

(iv) Status of Amendments

There was one (1) response filed on April 29, 2005, after final rejection of the claims on March 31, 2005, said Response having been considered by the Examiner.

(v) Summary Of Claimed Subject Matter

The subject invention relates to the filed of electronic security and the encryption and decryption of copy-protected material. Digital recording techniques are commonly used to record copy-protected content material such as audio and video recordings. Subsequent digital copies of such digital recordings are virtually indistinguishable from the original and offer the same quality as the original.

As the ease of illicitly providing high-quality reproductions of copy-protected content material increases, the need for preventing such reproductions increases.

The subject invention seeks to prevent a replay attack on a limited-use protection scheme. To that end, the subject invention, as claimed in claim 1, provides a recording medium 300 having a first memory 320 for storing encrypted content material 221 via a first write operation. This is shown in Fig. 1 and described in the

Substitute Specification on page 8, lines 14-15. The recording medium 300 also includes a recording indicator 310 for generating and storing a unique identifier 311 at each occurrence of the first write operation. This is described in the Substitute Specification on page 8, lines 14-15. In addition, the recording medium 300 includes a second memory 340 for storing, via a second write operation, a secure item 241 based on the unique identifier 311 when the encrypted content material 221 is stored, as described in the Substitute Specification on page 12, line 1 to page 13, line 14.

Claim 4 claims a rendering device 400 for rendering content material corresponding to the encrypted content material stored on the recording medium. In particular, the rendering device 400 includes one or more decrypters 420 for decrypting the encrypted content material 321 when the current unique identifier 312 corresponds to the original unique identifier 311, and a renderer 480 for rendering the content material. This is described in the Substitute Specification on page 12, line 15 to page 15, line 7. It should be understood that the original unique identifier 311 is derived from the secure item 341 read from the memory 340 in the recording medium and recovered by the decrypters 440 and 430.

Claim 8 claims a provider 200 of content material which includes a recorder for recording encrypted content material on a recording medium, the recorder comprising an input for receiving

content material 201, and a second input for receiving a content key 202, a first encrypter 220 for encrypting the content material 201 based on the content key 202, and means for writing the encrypted content material on the recording medium 300 in a first writing operation (Substitute Specification page 12, lines 1-3, page 8, lines 14-15, and page 9, lines 6-7). The recorder further includes a third input for receiving a unique identifier 311 from the recording medium 300 in response to the first writing operation, a second encrypter 210, 230, 240 for generating the secure item 241 based on the unique identifier 311, and means for writing the secure item 241 on the recording medium 300 in a second writing operation (Substitute Specification page 12, line 3 to page 13, line 14).

Claim 14 claims a method for providing content material and includes recording encrypted content material, dependent on content material and a content key, on a recording medium in a first write operation (Substitute Specification page 12, lines 1-3, and page 8, lines 14-15), and recording a secure item, dependent upon a unique identifier generated by and stored in the recording medium upon each first write operation, on the recording medium in a second write operation (Substitute Specification page 8, lines 14-15, and page 12, line 1 to page 13, line 14).

Finally, claim 18 claims a method of rendering content material, and includes determining a unique key based on the unique

identifier stored on the recording medium (Substitute Specification page 12, lines 15-18), decrypting the encrypted content key based on the unique key to provide a content key (Substitute Specification page 13, lines 14-19, and page 12, lines 22), decrypting the encrypted content material based on the content key (Substitute Specification page 12, lines 22-25), and rendering the content material (Substitute Specification page 15, lines 1-4).

(vi) Grounds of Rejection to be Reviewed on Appeal

Whether the invention, as claimed in claims 1-20, is unpatentable under 35 U.S.C. 103(a) over U.S. Patent 5,857,021 to Kataoka et al.

(vii) Arguments

(A) Claim 1-3.

The Kataoka et al. patent discloses a security system for protecting information stored in portable storage media in which a medium ID, a corporate ID and a terminal ID are used to protect the use of content material. In a particular embodiment described at col. 6, line 51 to col. 7, line 25, a first private key generating means 105 generates a private key, based on a medium ID 121 extracted from the storage medium and a unit ID 104 (e.g., a unique identifier of the computer system or of a portable drive unit). A first encrypting means 107 encrypts a data encryption key 106 with

the private key, and the encrypted data encryption key is written into the storage medium. A second encrypting means 108 encrypts the data to be stored with the date encryption key, and the encrypted data is written into the storage medium.

The Examiner states "Although the cited art does not specifically claim such a unique identifier being generated by the first write operation, Kataoke does discloses encvrypt8ing data through known algorithms or key generating means (e.g. col 7, ln 5-10, col. 5 ln 15-20). Thus steps need only be shuffled, reordered or repeated more time in order to obtain a unique identifier. Mere reordering or repeating of steps at different stages does not constitute new art."

Applicant submits that the Examiner has missed an impo9rtant feature of the subject invention. In particular, the Kataoka et al. data encoding system, shown in Fig. 9 therein, is described at col. 7, lines 10-26:

> "The first private key generating means 105 generates a private key, based on the medium ID 121 extracted from the storage medium 101 and a unit ID 104. The unit ID 104 is a unique identifier of the computer system itself or that of a portable drive unit (e.g., an MO drive). While the former identifier is normally used as the unit ID 104, the latter may be useful in some situations such as system installation or maintenance, because it is possible to install programs, set up data, and modify data using the same drive unit and storage medium for different computer systems. The first encrypting means 107 encrypts the data encryption key 106 with the private key generated by the first private key generating means 105. The encrypted encryption key is written into the storage medium 101 as the aforementioned permission data 122. The second

> encrypting means 108 encrypts the data with the data encryption key 106 and writes the encrypted data into the storage medium 101 as the aforementioned encrypted data 123."

Superficially, this may appear to be the same as the subject invention. However, it should be noted that the medium ID 121 "is an identifier uniquely assigned to the storage medium 101, which is burned into a predetermined region in a non-rewritable manner with a laser beam, for example" (col. 6, lines 64-67). As such, no matter how many different times encrypted data is to be stored on the storage medium 101, the same medium ID 121 is used to encrypt the encryption key for storage on the storage medium 101.

In the subject invention, on the other hand, a recording medium comprises "a recording indicator for generating and storing a unique identifier at each occurrence of the first write operation". As described in the Substitute Specification on page 8, paragraph [0014], "A new number U (unique identifier) is created each time encrypted content material 221 is stored to the memory area 320 of the medium 300." Hence, the recording medium contains a, for example, number generator for generating and storing a new unique identifier each time encrypted content material is stored in a first memory of the recording medium via a first write operation. The content provider 200 then receives this unique identifier and the unique identifier to encrypt the encryption key used to encrypt the encrypted content material. This encrypted encryption key

(secure item) is then written into a second memory of the recording medium via a second write operation.

Applicant submits that Kataoka et al. teaches away from the subject invention in that Kataoka et al. goes to great lengths to make sure that the medium ID is unchangeable, while, in the subject invention, the unique identifier changes for each first write operation.

It appears that the Examiner dismisses this feature by indicating that Kataoka et al. "discloses encrypting data through known algorithms or key generating means", and then stating that mere reordering or repeating of steps at different stages does not constitute new art. However, Applicant submits that the subject invention does not merely reorder or repeat steps taken by Kataoka et al. at different stages. Rather, the subject invention adds a new level of security.

Applicant understands that there are numerous different algorithms which can be used for encryption, and Applicant is not trying to come up with a new algorithm for encrypting the content material, or for encrypting the encryption key used to encrypt the content material. Nor is Applicant trying to come up with an additional key generator to be used in the content provider 200 (i.e., recording device). Rather, Applicant has found that an added level of security is achieved when the recording medium comprises "a recording indicator for generating and storing a unique

identifier at each occurrence of the first write operation" (i.e., the storing of encrypted content material in a first memory of the recording medium), this unique identifier being used to form a secure item which is stored in a second memory of the recording medium via a second write operation when the encrypted content material is stored.

(B) Claims 4-7.

The Examiner states "Kataoka discloses a first decrypting means and second decrypting means which provide the content material only when the current value of the recording indicator corresponds to its original value. (e.g. Col 2 ln 13-34). Although the cited art does not specifically claim such a unique identifier being generated by the first write operation, Kataoke does discloses encrypting data through known algorithms or key generating means (e.g. col 7 ln 5-10. col 5 ln 15-20). Thus steps need only be shuffled, reordered or repeated more time in order obtain a unique identifier. Mere reordering or repeating of steps at different stages does not constitute new art."

Again, Applicant submits that the Examiner is mistaken. In particular the portion of Kataoka et al. cited by the Examiner states:

> "The security control unit comprises four elements. First private key generating means generates a private key based on the medium identifier extracted from the storage medium and the unit identifier, when the

> security control unit attempts to write data into the storage medium. First encrypting means produces permission data by encrypting a data encryption key with the private key generated by the first private key generating means, and it writes the permission data into the storage medium. Second encrypting means encrypts the data with the data encryption key, and writes the encrypted data into the storage medium. When the security control unit attempts to retrieve the encrypted data written in the storage medium, second private key generating means regenerates the private key based on the medium identifier extracted from the storage medium and the unit identifier. First decrypting means produces a data decryption key by decrypting the permission data extracted from the storage medium, with the private key regenerated by the second private key generating means. Second decrypting means decrypts the encrypted data extracted from the storage medium, with the data decryption key produced by the first decrypting means."

Claim 4 recites, in part "the recording medium also including a recording indicator for generating and storing an original unique identifier and a current unique identifier depending upon first write operations of said encrypted content material being written into the recording medium". With regard to claim 4, since the current unique identifier changes with each first write operation, the recording medium further stores the original unique identifier, and a rendering device only "allows" the one or more decrypters to provide the content material when the original unique identifier of the recording indicator corresponds to the current unique identifier of the recording indicator. Applicant submits that the above passage of Kataoka et al. neither shows nor suggests this comparison. In fact, since the medium ID on the storage medium of Kataoka et al. never changes, there is no need in Kataoka et al.,

and as such, no disclosure or suggestion of the generation and storage of the original unique identifier of the recording indicator, the generation and storage of the current unique identifier of the recording indicator, and the comparison of the stored current unique identifier and the original unique identifier.

(C) Claims 8-17.

The Examiner states "Kataoka recording encrypted content material on a medium dependent on the content material and a content key (e.g. col 7 ln 23-26) and further discloses recording a secure item (encrypted encryption key) which is encrypted using a private key that is generated using based on a recording indicator that is associated with the recording medium (medium ID and Unit ID)(e.g. col 7 ln 9-12). Although the cited art does not specifically claim such a unique identifier being generated by the first write operation, Kataoke does discloses encrypting data through known algorithms or key generating means (e.g. col 7 ln 5-10. col 5 ln 15-20). Thus steps need only be shuffled, reordered or repeated more time in order obtain a unique identifier. Mere reordering or repeating of steps at different stages does not constitute new art."

While Kataoka et al. discloses recording a secure item which is encrypted using a private key that is generated based on the

medium Id that is associated with the recording medium, Applicant submits that this is not what is claimed in, for example, claim 8. In particular, claim 8 states "a third input for receiving a unique identifier from the recording medium in response to the first writing operation, said recording medium having a recording indicator for generating and storing a unique identifier at each occurrence of a first writing operation". As such, the unique identifier is not merely associated with the recording medium, but is generated each time by the recording indicator of the recording medium at each occurrence of a first writing operation. It should be appreciated that the same "unique identifier" is not generated by the recording indicator of the recording medium at each occurrence of a first writing operation. Rather, a unique identifier is generated by the recording indicator of the recording medium at each occurrence of a first writing operation. The use of the term "a" in the claim is significant in that it indicates that a different unique identifier is generated each time.

(D) Claims 18-20.

The Examiner states "Kataoka discloses a claimed unique key that is the private key, the encrypted content key is decrypted using this private key, and then the encrypted content is decrypted using the content key (e.g. Col 2 ln 13-34). Although the cited art does not specifically claim such a unique identifier being

generated by the first write operation, Kataoke does discloses encrypting data through known algorithms or key generating means (e.g. col 7 ln 5-10. col 5 ln 15-20). Thus steps need only be shuffled, reordered or repeated more time in order obtain a unique identifier. Mere reordering or repeating of steps at different stages does not constitute new art."

The Examiner appears to be repeatedly overlooking an important aspect of the subject invention, i.e., the unique key being based on the unique identifier, and that a unique identifier is generated by and stored on the recording medium each time encrypted content material is recorded on the recording medium. If a user tried to make an unauthorized copy of a recording medium containing the encrypted content material and the encrypted content key onto another recording medium, then the unique identifier generated in the another recording medium and supplied to the rendering device would be different from the unique identifier used to encrypt the content key. As such, the supplied unique identifier would not enable the decrypting of the encrypted content material.

Based on the above arguments, Appellant believes that the subject invention is not rendered obvious by the prior art and is patentable thereover. Therefore, Appellant respectfully requests that this Board reverse the decisions of the Examiner and allow this application to pass on to issue.

Respectfully submitted,

by _____
Edward W. Goodman, Reg. 28,613
Attorney

CERTIFICATE OF MAILING

It is hereby certified that this correspondence is being deposited with the United States Postal Service as first-class mail in an envelope addressed to:

COMMISSIONER OF PATENTS AND TRADEMARKS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

On August 15, 2005

By Barnett Jones

(viii) Appendix

CLAIMS ON APPEAL

1. (Previously Presented) A recording medium comprising:

a first memory for storing encrypted content material via a first write operation;

a recording indicator for generating and storing a unique identifier at each occurrence of the first write operation; and

a second memory for storing, via a second write operation, a secure item based on the unique identifier when the encrypted content material is stored.

2. (Previously Presented) The recording medium as claimed in claim 1, wherein:

the secure item includes an encrypted key for facilitating a decryption of the encrypted content material, the encrypted key being dependent upon the unique identifier.

3. (Previously Presented) The recording medium as claimed in claim 1, wherein:

the recording indicator includes a counter incremented by a recording device when the recording device records the encrypted content material.

4. (Previously Presented) A rendering device for rendering content material corresponding to encrypted content material contained on a recording medium, the recording medium also including a recording indicator for generating and storing an original unique identifier and subsequently a current unique identifier in response to first write operations of said encrypted content material being written into the recording medium, the rendering device comprising:

one or more decrypters for decrypting the encrypted content material based on a current value of the recording indicator, said one or more decrypters provide the content material only when the current unique identifier of the recording indicator corresponds to the original unique identifier of the recording indicator; and

a renderer configured to render the content material.

5. (Previously Presented) The rendering device as claimed in claim 4, wherein said rendering device further comprises:

an authorization device for controlling the renderer based on a usage-measure associated with the recording medium, and a validity period associated with the content material.

6. (Previously Presented) The rendering device as claimed in claim 4, wherein said rendering device further comprises:

a key generator for creating a unique key based on the current value of the recording indicator,

and wherein the one or more decrypters decrypt the encrypted content material based on the unique key based on the current unique identifier of the recording indicator.

7. (Previously Presented) The rendering device as claimed in claim 6, wherein the one or more decrypters include:

a first decrypter for decrypting a doubly encrypted content key based on a private key of the rendering device to provide a singly encrypted content key;

a second decrypter for decrypting the singly encrypted content key based on the unique key that is based on the current unique identifier of the recording indicator to provide a content key; and

a third decrypter for decrypting the encrypted content material based on the content key to provide the content material.

8. (Previously Presented) A provider of content material comprising:

a recorder for recording encrypted content material and a corresponding secure item on a recording medium, said recorder comprising:

a first input for receiving content material;

a second input for receiving a content key;

a first encrypter for encrypting the content material based on the content key;

means for writing the encrypted content material on the recording medium in a first writing operation;

a third input for receiving a unique identifier from the recording medium in response to the first writing operation, said recording medium having a recording indicator for generating and storing a unique identifier at each occurrence of a first writing operation;

a second encrypter for generating the secure item based on the unique identifier received from the recording medium; and

means for writing the secure item on the recording medium in a second writing operation.

9. (Previously Presented) The content material provider as claimed in claim 8, wherein the content material provider further comprises:

an allocator for allocating rendering rights associated with the encrypted content material,

and wherein the recorder further records the rendering rights on the recording medium.

10. (Previously Presented) The content material provider as claimed in claim 8, wherein

the secure item corresponds to an encryption of the content key based on the unique identifier.

11. (Previously Presented) The content material provider as claimed in claim 8, wherein said content material provider further comprises:

one or more encrypters for providing the secure item.

12. (Previously Presented) The content material provider as claimed in claim 8, wherein said content material provider further comprises:

a key generator for generating a unique key based on the unique identifier; and

one or more encrypters for encrypting the content key based on the unique key to produce the secure item.

13. (Previously Presented) The content material provider as claimed in claim 8, wherein said content material provider further comprises:

a first encrypter for encrypting the content key based on a unique key that is dependent upon the unique identifier to produce a singly encrypted content key; and

a second encrypter for encrypting the singly encrypted content key based on a public key that is associated with a rendering device to produce a doubly encrypted content key corresponding to the secure item.

14. (Previously Presented) A method of providing content material, the method comprising the steps:

recording encrypted content material on a recording medium in a first write operation, the encrypted content material being dependent upon the content material and a content key; and

recording a secure item on the recording medium in a second write operation, the secure item being dependent upon a unique identifier generated by and stored in the recording medium upon each first write operation.

15. (Previously Presented) The method as claimed in claim 14, wherein said method further comprises the step:

recording rendering rights associated with the encrypted content material on the recording medium.

16. (Previously Presented) The method as claimed in claim 14, wherein said method further comprises the steps:

generating a unique key based on the unique identifier; and

encrypting the content key using the unique key to produce the secure item.

17. (Previously Presented) The method as claimed in claim 14, wherein the method further comprises the steps:

generating a unique key based on the unique identifier;

encrypting the content key using the unique key to produce a singly encrypted content key; and

encrypting the singly encrypted content key using a public key associated with a rendering device to produce the secure item.

18. (Previously Presented) A method of rendering content material from a recording medium that includes encrypted content material, an encrypted content key, and a unique identifier generated by and stored on the recording medium each time said encrypted content material is recorded on said recording medium, the method comprising the steps:

determining a unique key based on the unique identifier;

decrypting the encrypted content key based on the unique key to provide a content key;

decrypting the encrypted content material based on the content key to provide the content material; and

rendering the content material.

19. (Previously Presented) The method as claimed in claim 18, wherein:

the recording medium also includes rendering rights, and

the step of rendering the content material is dependent upon the rendering rights.

20. (Previously Presented) The method as claimed in claim 18, wherein the step of decrypting the encrypted content key includes:

decrypting the encrypted content key based on a private key to provide a singly encrypted content key; and

decrypting the singly encrypted content key based on the unique key to provide the content key.

(ix) Evidence Appendix

There is no evidence which had been submitted under 37 C.F.R. 1.130, 1.131 or 1.132, or any other evidence entered by the Examiner and relied upon by Appellant in this Appeal.

(x) Related Proceedings Appendix

Since there were no proceedings identified in section (ii) herein, there are no decisions rendered by a court or the Board in any proceeding identified pursuant to paragraph (c)(1)(ii) of 37 C.F.R. 41.37.

AF
$ 3621
JFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of — Atty. Docket

MICHAEL A. EPSTEIN — PHA 23,637

Serial No.: 09/454,349 — Group Art Unit: 3621

Filed: December 3, 1999 — Examiner: C.O. Sherr

Title: KEY DISTRIBUTION VIA A MEMORY DEVICE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Enclosed is an original copy of an Appeal Brief in the above-identified patent application.

Please charge the fee of $500.00 to Deposit Account No. 14-1270.

Respectfully submitted,

08/18/2005 SHASSEN1 00000021 141270 09454349
01 FC:1402 500.00 DA

By _____
Edward W. Goodman, Reg. 28,613
Attorney
(914) 333-9611

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited this date with the United States Postal Service as first-class mail in an envelope addressed to:

COMMISSIONER OF PATENTS AND TRADEMARKS
P.O. BOX 1450, ALEXANDRIA, VA 22313-1450

On August 15, 2005
(Date of Mailing)

By Burnett Jones
(Signature)